

Predicting zero reductions in Gröbner basis computations

Christian Eder*

c/o Department of Mathematics

University of Kaiserslautern

67653 Kaiserslautern, Germany

ederc@mathematik.uni-kl.de

April 2, 2014

Abstract

Since Buchberger's initial algorithm for computing Gröbner bases in 1965 many attempts have been taken to detect zero reductions in advance. Buchberger's Product and Chain criteria may be known the most, especially in the installation of Gebauer and Möller. A relatively new approach are signature-based criteria which were first used in Faugère's **F5** algorithm in 2002. For regular input sequences these criteria are known to compute no zero reduction at all. In this paper we give a detailed discussion on zero reductions and the corresponding syzygies. We explain how the different methods to predict them compare to each other and show advantages and drawbacks in theory and practice. With this a new insight into algebraic structures underlying Gröbner bases and their computations might be achieved.

1 Introduction

Since 1965 [3] Gröbner bases are practically feasible. Besides theoretical studies and generalizations, see, for example, [21, 25, 24, 26], one of the main algorithmic improvements is the prediction of useless data during the computations. That means to use criteria to detect zero reductions in advance

*The author was supported by the EXACTA grant (ANR-09-BLAN-0371-01) of the French National Research Agency.

[4, 5]. Gebauer and Möller gave an optimal implementation of Buchberger’s criteria [18], but showed that not all zero reductions are discarded. In 2002 Faugère presented the **F5** algorithm [11] which uses new criteria based on so-called “signatures”. For regular input sequences **F5** does not compute any zero reduction at all. Over the years optimized variants of **F5** were presented, see, for example, [8, 1, 13, 14, 30, 10]. Still, not much is known about the connection between Buchberger’s criteria and those being based on signatures. Do they cover each other? How do they behave in different situations? In [16, 17] Gash gave only a small note on possible combinations of both attempts in very specific cases. In [19] Gerdt and Hashemi have considered the usage of Buchberger’s criteria in the **G2V** algorithm, i.e. restricted to a signature-based algorithm using an incremental structure computing the Gröbner basis. Gao, Volny and Wang have added corresponding step to the 2013 revision of **GVW** (see [15]).

Here we present a detailed discussion on the connection between different attempts to predict zero reductions in Gröbner basis computations. After a short introduction to our notation in which we also introduce a generic signature-based algorithm denoted **RB** that mirrors Buchberger’s algorithm, we explain in Section 3 Buchberger’s Product and Chain criteria as well as the Syzygy and Rewritten criteria of **RB**. We show that in general signature-based criteria predict more zero reductions, but with the drawback of introducing a more restricted reduction process called “ \mathfrak{s} -reduction” (see Definition 2.3). In Section 4 we explain how the Rewritten criterion can be improved. Following that we show that the Rewritten criterion includes the Chain criterion and we give a vivid presentation of this fact in Example 5.1. Section 6 discusses why the Product criterion is, in general, not completely covered by signature-based criteria. Proving that we can safely use the Product criterion in **RB** enables us to present an optimized variant which introduces this criterion without overhead. As we see in Section 8 situations where syzygies coming from the Product criterion improve computations are very rare. Even more, we give a conjecture that for a specific module monomial order on the signatures all syzygies coming from the Product criterion are already known in **RB**.

Dear reader, please note that in here is no intention to introduce a new, more efficient variant of already known signature-based Gröbner basis algorithms. This paper should be understood as a first step in understanding the connections between different attempts to minimize the number of useless data in Gröbner basis computations. This might lead to a better exploitation of, until now, unused underlying algebraic structures in order to improve computations even further.

2 Notations

In this section we introduce notations and basic terminology used in this publication. Readers familiar with signature-based algorithms might skip this section. We extend the notation introduced in [10].

Let \mathcal{R} be a polynomial ring over a field \mathcal{K} . All polynomials $f \in \mathcal{R}$ can be uniquely written as a finite sum $f = \sum_{\kappa_v, x^v \in \mathcal{M}} \kappa_v x^v$ where $\kappa_v \in \mathcal{K}$, $x^v := \prod_i x_i^{v_i}$ and \mathcal{M} is minimal. The elements of \mathcal{M} are the *terms* of f . The *support* of f is defined by $\text{sup}(f) := \{\text{terms in } f\}$. A *monomial* is a polynomial with exactly one term. A monomial with a coefficient of 1 is *monic*. Neither monomials nor terms of polynomials are necessarily monic. We write $f \simeq g$ for $f, g \in \mathcal{R}$ if there exists a non-zero $\kappa \in \mathcal{K}$ such that $f = \kappa g$.

Let \mathcal{R}^m be a free \mathcal{R} -module and let e_1, \dots, e_m be the canonical basis of unit vectors in \mathcal{R}^m . $\alpha \in \mathcal{R}^m$ can be uniquely written as a finite sum $\alpha = \sum_{ae_i \in \mathcal{N}} ae_i$ where the a are monomials and \mathcal{N} is minimal. The elements of \mathcal{N} are the *terms* of α . A *module monomial* is an element of \mathcal{R}^m with exactly one term. A module monomial with a coefficient of 1 is *monic*. Neither module monomials nor terms of module elements are necessarily monic. Let $\alpha \simeq \beta$ for $\alpha, \beta \in \mathcal{R}^m$ if $\alpha = \kappa \beta$ for some non-zero $\kappa \in \mathcal{K}$.

Let \leq denote two different orders – one for \mathcal{R} and one for \mathcal{R}^m : The order for \mathcal{R} is a monomial order, which means that it is a well-order on the set of monomials in \mathcal{R} such that $a \leq b$ implies $ca \leq cb$ for all monomials $a, b, c \in \mathcal{R}$. The order for \mathcal{R}^m is a module monomial order which means that it is a well-order on the set of module monomials in \mathcal{R}^m such that $S \leq T$ implies $cS \leq cT$ for all module monomials $S, T \in \mathcal{R}^m$ and monomials $c \in \mathcal{R}$. We require the two orders to be *compatible* in the sense that $a \leq b$ if and only if $ae_i \leq be_i$ for all monomials $a, b \in \mathcal{R}$ and $i = 1, \dots, m$. Consider a finite sequence of polynomials $f_1, \dots, f_m \in \mathcal{R}$ called the *input (polynomials)*. We call f_1, \dots, f_m a regular sequence if f_i is a non-zero-divisor on $\mathcal{R} / \langle f_1, \dots, f_{i-1} \rangle$ for $i = 2, \dots, m$. We define the homomorphism $\alpha \mapsto \overline{\alpha}$ from \mathcal{R}^m to \mathcal{R} by $\overline{\alpha} := \sum_{i=1}^m \alpha_i f_i$. An element $\alpha \in \mathcal{R}^m$ with $\overline{\alpha} = 0$ is called a *syzygy*. The module of all syzygies of f_1, \dots, f_m is denoted by $\text{syz}(f_1, \dots, f_m)$.

The following compatible module monomial orders are commonly used in signature-based Gröbner basis algorithms.

Definition 2.1. Let $<$ be a monomial order on \mathcal{R} and let ae_i, be_j be two module monomials in \mathcal{R}^m .

- (a) $ae_i <_{\text{pot}} be_j$ iff $i < j$ or $i = j$ and $a < b$.
- (b) $ae_i <_{\text{top}} be_j$ iff $a < b$ or $a = b$ and $i < j$.

These two orders can be combined by either a weighted degree or a weighted leading monomial:

- (c) $ae_i <_{\text{d-pot}} be_j$ iff $\deg(\overline{ae_i}) < \deg(\overline{be_j})$ or $\deg(\overline{ae_i}) = \deg(\overline{be_j})$ and

- $ae_i <_{\text{pot}} be_j$. Similar we define $ae_i <_{\text{d-top}} be_j$.
- (d) $ae_i <_{\text{lt-pot}} be_j$ iff $\text{lt}(\overline{ae_i}) < \text{lt}(\overline{be_j})$ or $\text{lt}(\overline{ae_i}) = \text{lt}(\overline{be_j})$ and $ae_i <_{\text{pot}} be_j$.
Similar we define $ae_i <_{\text{lt-top}} be_j$.

Note that some of these orders are not efficient for signature-based Gröbner basis computations (see, for example, [14]). Here we concentrate on $<_{\text{pot}}$, $<_{\text{d-pot}}$ and $<_{\text{lt-pot}}$. Note that changing $i < j$ to $-i < -j$ in the above definition of $<_{\text{pot}}$ we receive the module order used in [11] for the **F5** algorithm.

Next we introduce the notion of signatures. Note the connections and relations to structures in the plain polynomial setting.

Definition 2.2.

- (a) The *lead term* $\text{lt}(f)$ of $f \in \mathcal{R} \setminus \{0\}$ is the \leq -maximal term of f . The *lead coefficient* $\text{lc}(f)$ of f is the coefficient of $\text{lt}(f)$. For a set $F \subset \mathcal{R}$ we define the *lead ideal* of F by $L(F) := \langle \text{lt}(f) \mid f \in F \rangle$.
- (b) The *lead term* resp. *signature* $\mathfrak{s}(\alpha)$ of $\alpha \in \mathcal{R}^m \setminus \{0\}$ denotes the \leq -maximal term of α . If $ae_i = \mathfrak{s}(\alpha)$ then we call $\text{ind}(\alpha) := i$ the *index* of α . For a set $M \in \mathcal{R}^m$ we define the *lead module* of M by $L(M) := \langle \text{lt}(\alpha) \mid \alpha \in M \rangle$.
- (c) For $\alpha \in \mathcal{R}^m$ the *sig-poly pair* of α is $(\mathfrak{s}(\alpha), \overline{\alpha}) \in \mathcal{R}^m \times \mathcal{R}$.
- (d) $\alpha, \beta \in \mathcal{R}^m$ are *equal up to sig-poly pairs* if $\mathfrak{s}(\alpha) = \mathfrak{s}(\kappa\beta)$ and $\overline{\alpha} = \overline{\kappa\beta}$ for some non-zero $\kappa \in \mathcal{K}$. Correspondingly, α, β are said to be *equal up to sig-lead pairs* if $\mathfrak{s}(\alpha) = \mathfrak{s}(\kappa\beta)$ and $\text{lt}(\overline{\alpha}) = \text{lt}(\overline{\kappa\beta})$ for some non-zero $\kappa \in \mathcal{K}$.

Next we introduce the notion of Gröbner bases. Let $f \in \mathcal{R}$ and let t be a term of f . Then we can *reduce* t by $g \in \mathcal{R}$ if there exists a monomial b such that $\text{lt}(bg) = t$. The outcome of the reduction step is $f - bg$ and g is called the *reducer*. When g reduces t we also say that bg reduces f . That way b is introduced implicitly instead of having to repeat the equation $\text{lt}(bg) = t$.

The result of an reduction of $f \in \mathcal{R}$ is an element $h \in \mathcal{R}$ that has been calculated from f by a sequence of reduction steps. Thus, reductions can always be assumed to be done w.r.t. some finite subset $G \subset \mathcal{R}$.

Let $I = \langle f_1, \dots, f_m \rangle$ be an ideal in \mathcal{R} . A finite subset G of \mathcal{R} is a *Gröbner basis up to degree d* for I if $G \subset I$ and for all $f \in I$ with $\deg(f) \leq d$ f reduces to zero w.r.t. G . G is a *Gröbner basis* for I if G is a Gröbner basis in all degrees.

In the very same way one can define Gröbner basis with the notion of standard representations: Let $f \in \mathcal{R}$ and $G \subset \mathcal{R}$ finite. A representation $f = \sum_{i=1}^k m_i g_i$ with monomials $m_i \neq 0$, $g_i \in G$ pairwise different is called a *standard representation* if $\max_{\leq} \{\text{lt}(m_i g_i) \mid 1 \leq i \leq k\} \leq \text{lt}(f)$. If for any $f \in \langle G \rangle$ with $f \neq 0$ f has a standard representation w.r.t. G and \leq then G is a Gröbner basis for $\langle G \rangle$. Moreover, note that the existence of a standard representation does not imply reducibility to zero, see, for example, Exercise 5.63 in [2]).

Moreover, Buchberger gave an algorithmic description of Gröbner bases using the notion of so-called S-polynomials:

Let $f \neq 0, g \neq 0 \in \mathcal{R}$ and let $\lambda = \text{lcm}(\text{lt}(f), \text{lt}(g))$ be the monic least common multiple of $\text{lt}(f)$ and $\text{lt}(g)$. The *S-polynomial* between f and g is given by

$$\text{spol}(f, g) := \frac{\lambda}{\text{lt}(f)}f - \frac{\lambda}{\text{lt}(g)}g.$$

Theorem 2.1 (Buchberger's criterion). *Let $I = \langle f_1, \dots, f_m \rangle$ be an ideal in \mathcal{R} . A finite subset G of \mathcal{R} is a Gröbner basis for I if $G \subset I$ and for all $f, g \in G$ $\text{spol}(f, g)$ reduces to zero w.r.t. G .*

Every non-syzygy module element $\alpha \in \mathcal{R}^m$ has two main associated characteristics – the signature $\mathfrak{s}(\alpha) \in \mathcal{R}^m$ and the lead term $\text{lt}(\overline{\alpha}) \in \mathcal{R}$ of its image $\overline{\alpha}$. Lead terms and signatures include a coefficient for mathematical convenience, though an implementation of a signature-based Gröbner basis algorithm working in polynomial rings over fields need not store the signature coefficients.

In order to keep track of the signatures when reducing corresponding polynomial data we get a classic polynomial reduction together with a further condition.

Definition 2.3. Let $\alpha \in \mathcal{R}^m$ and let t be a term of $\overline{\alpha}$. Then we can *s-reduce* t by $\beta \in \mathcal{R}^m$ if

- (a) there exists a monomial b such that $\text{lt}(\overline{b\beta}) = t$ and
- (b) $\mathfrak{s}(b\beta) \leq \mathfrak{s}(\alpha)$.

The outcome of the *s-reduction* step is then $\alpha - b\beta$ and β is called the *s-reducer*. When β *s-reduces* t we also say for convenience that $b\beta$ *s-reduces* α . That way b is introduced implicitly instead of having to repeat the equation $\text{lt}(\overline{b\beta}) = t$.

Remark 2.1. Note that Condition (a) from Definition 2.3 defines a classic polynomial reduction step. It implies that $\text{lt}(\overline{b\beta}) \leq \text{lt}(\overline{\alpha})$. Moreover, Condition (b) lifts the above implication to \mathcal{R}^m so that it involves signatures. Since we are interested in computing Gröbner bases in \mathcal{R} one can interpret an *s-reduction* of α by β as classic polynomial reduction of $\overline{\alpha}$ by $\overline{\beta}$ together with Condition (b). Thus an *s-reduction* represents a connection between data in \mathcal{R} and corresponding data in \mathcal{R}^m when a polynomial reduction takes place.

Just as for classic polynomial reduction, if $\text{lt}(\overline{b\beta}) \simeq \text{lt}(\overline{\alpha})$ then the *s-reduction* step is a *top s-reduction step* and otherwise it is a *tail s-reduction step*. Analogously we define the distinction for signatures: If $\mathfrak{s}(b\beta) \simeq \mathfrak{s}(\alpha)$ then the reduction step is a *singular s-reduction step* and otherwise it is a *regular s-reduction step*.

The result of an *s-reduction* of $\alpha \in \mathcal{R}^m$ is $\gamma \in \mathcal{R}^m$ that has been calculated from α through a sequence of *s-reduction* steps such that γ cannot be further

\mathfrak{s} -reduced. The reduction is a *tail \mathfrak{s} -reduction* if only tail \mathfrak{s} -reduction steps are allowed and it is a *top \mathfrak{s} -reduction* if only top \mathfrak{s} -reduction steps are allowed. The reduction is a *regular \mathfrak{s} -reduction* if only regular \mathfrak{s} -reduction steps are allowed. $\alpha \in \mathcal{R}^m$ is *\mathfrak{s} -reducible* if it can be \mathfrak{s} -reduced.

If α \mathfrak{s} -reduces to γ and γ is a syzygy then we say that α *\mathfrak{s} -reduces to zero* even if $\gamma \neq 0$.

Note that analogously to the classic polynomial reduction \mathfrak{s} -reduction is always with respect to a finite basis $\mathcal{G} \subset \mathcal{R}^m$. The \mathfrak{s} -reducers in \mathfrak{s} -reduction are chosen from the basis \mathcal{G} .

Definition 2.4. Let $I = \langle f_1, \dots, f_m \rangle$ be an ideal in \mathcal{R} . A finite subset $\mathcal{G} \subset \mathcal{R}^m$ is a *signature Gröbner basis in signature T* for I if all $\alpha \in \mathcal{R}^m$ with $\mathfrak{s}(\alpha) = T$ \mathfrak{s} -reduce to zero w.r.t. \mathcal{G} . \mathcal{G} is a *signature Gröbner basis up to signature T* for I if \mathcal{G} is a signature Gröbner basis in all signatures S such that $S < T$. \mathcal{G} is a *signature Gröbner basis* for I if it is a signature Gröbner basis for I in all signatures. We denote $\overline{\mathcal{G}} := \{\overline{\alpha} \mid \alpha \in \mathcal{G}\} \subset \mathcal{R}$.

Lemma 2.1. Let $I = \langle f_1, \dots, f_m \rangle$ be an ideal in \mathcal{R} . If \mathcal{G} is a signature Gröbner basis for I then $\overline{\mathcal{G}}$ is a Gröbner basis for I .

Proof. For example, see Section 2.2 in [30]. □

Convention 2.1. In the following, when denoting $\mathcal{G} \subset \mathcal{R}^m$ “a signature Gröbner basis (up to signature T)” we always mean “a signature Gröbner basis (up to signature T) for $I = \langle f_1, \dots, f_m \rangle$ ”. We omit the explicit notion of the input ideal whenever it is clear from the context. The same holds for classic Gröbner bases $G \subset \mathcal{R}$.

As in the classic polynomial setting we want to give an algorithmic description of signature Gröbner bases. For this we introduce the notion of S-pairs.

Definition 2.5.

- (a) Let $\alpha, \beta \in \mathcal{R}^m$ such that $\overline{\alpha} \neq 0, \overline{\beta} \neq 0$ and let the monic least common multiple of $\text{lt}(\overline{\alpha})$ and $\text{lt}(\overline{\beta})$ be $\lambda = \text{lcm}(\text{lt}(\overline{\alpha}), \text{lt}(\overline{\beta}))$. The *S-pair* between α and β is given by

$$\text{spair}(\alpha, \beta) := \frac{\lambda}{\text{lt}(\overline{\alpha})} \alpha - \frac{\lambda}{\text{lt}(\overline{\beta})} \beta.$$

- (b) $\text{spair}(\alpha, \beta)$ is *singular* if $\mathfrak{s}\left(\frac{\lambda}{\text{lt}(\overline{\alpha})} \alpha\right) \simeq \mathfrak{s}\left(\frac{\lambda}{\text{lt}(\overline{\beta})} \beta\right)$. Otherwise it is *regular*.

Note that $\text{spair}(\alpha, \beta) \in \mathcal{R}^m$ and $\overline{\text{spair}(\alpha, \beta)} = \text{spol}(\overline{\alpha}, \overline{\beta})$.

Theorem 2.2. *Let T be a module monomial of \mathcal{R}^m and let $\mathcal{G} \subset \mathcal{R}^m$ be a finite basis. Assume that all regular S-pairs $\text{spair}(\alpha, \beta)$ with $\alpha, \beta \in \mathcal{G}$ and $\mathfrak{s}(\text{spair}(\alpha, \beta)) < T$ \mathfrak{s} -reduce to zero and all e_i with $e_i < T$ \mathfrak{s} -reduce to zero. Then \mathcal{G} is a signature Gröbner basis up to signature T .*

Proof. For example, see Theorem 2 in [31]. □

Note the similarity of Theorem 2.2 and Theorem 2.1. The outcome of classic polynomial reduction depends on the choice of reducer which can change what the intermediate bases are in the classic Buchberger algorithm. Lemma 2.2 implies that all S-pairs with the same signature yield the same regular \mathfrak{s} -reduced result as long as we process S-pairs in order of increasing signature.

Lemma 2.2. *Let $\alpha, \beta \in \mathcal{R}^m$ and let \mathcal{G} be a signature Gröbner basis up to signature $\mathfrak{s}(\alpha) = \mathfrak{s}(\beta)$. If α and β are both regular top \mathfrak{s} -reduced then $\text{lt}(\bar{\alpha}) = \text{lt}(\bar{\beta})$ or $\bar{\alpha} = \bar{\beta} = 0$. Moreover, if α and β are both regular \mathfrak{s} -reduced then $\bar{\alpha} = \bar{\beta}$.*

Proof. For example, see Lemma 3 in [31]. □

We simplify notations using facts from the previous statements.

Notation 2.1.

- (a) Due to Lemma 2.2 we assume in the following that \mathcal{G} always denotes a finite subset of \mathcal{R}^m with the property that for $\alpha, \beta \in \mathcal{G}$ with $\mathfrak{s}(\alpha) \simeq \mathfrak{s}(\beta)$ it follows that $\alpha = \beta$.
- (b) Theorem 2.2 suggests to consider only regular S-pairs for the computation of signature Gröbner bases. Thus in the following “S-pair” always refers to “regular S-pair”.

3 Detecting zero reductions

Different criteria to predict useless data during the computation of a Gröbner basis exist. One such attempt goes back to Buchberger and implements two criteria.

Lemma 3.1 (Product criterion [3, 4]). *Let $f, g \in \mathcal{R}$ with $\text{lcm}(\text{lt}(f), \text{lt}(g)) = \text{lt}(f) \text{lt}(g)$. Then $\text{spol}(f, g)$ reduces to zero w.r.t. $\{f, g\}$.*

In the above situation we also say that the S-polynomial $\text{spol}(f, g)$ fulfills the *Product criterion*.

Lemma 3.2 (Chain criterion [23, 4]). *Let $f, g, h \in \mathcal{R}$, $G \subset \mathcal{R}$ finite. If $\text{lt}(h) \mid \text{lcm}(\text{lt}(f), \text{lt}(g))$, and if $\text{spol}(f, h)$ and $\text{spol}(h, g)$ have a standard representation w.r.t. G resp., then $\text{spol}(f, g)$ has a standard representation w.r.t. G .*

In the above situation we also say that the triple $(f, g, h) \in \mathcal{R}^3$ fulfills the *Chain criterion*. Another formulation of Lemma 3.2 (also explaining its name) is the relation

$$\text{spol}(f, g) = u \text{spol}(f, h) + v \text{spol}(h, g) \quad (1)$$

for suitable $u, v \in \mathcal{M}$. Clearly, if we know the standard representations of $\text{spol}(f, h)$ and $\text{spol}(h, g)$, respectively, $\text{spol}(f, g)$ does not need to be considered when computing G . Depending on u and v we may even be free to remove any of the three above mentioned S-polynomials from the Gröbner basis computation as long as we guarantee to consider the other two, for more details on this we refer to [18].

Gebauer and Möller present in [18] a very efficient implementation of a combination of the Product and the Chain criterion in a Buchberger-like algorithm to compute Gröbner bases.¹

In 2002 Faugère published the **F5** algorithm, the first Gröbner basis algorithm using signatures to predict zero reductions. In the last years many researchers have contributed to optimize and generalize this attempt, for example [22, 13, 1, 9, 14, 32, 30, 31, 10, 29].

We can give a general description of signature-based Gröbner basis algorithms, denoted **RB**, similar to Buchberger's algorithm in Algorithm 1. It depends on the algorithm **Rewritable** which implements the Rewritten criterion (Lemma 3.3).

In the following we focus on the rewritability of elements and the generation of syzygies in order to detect useless zero reductions. We refer to [30, 10] for other details of **RB**.

Until now **UpdateSyz** in Line 14 is just a placeholder for a generic subalgorithm. In Section 4 we make use of **UpdateSyz** in order to improve the detection of zero reductions.

Next we state the main signature-based criterion to remove useless data.

Lemma 3.3 (Rewritten criterion). *For signature T **RB** needs to handle exactly one $a\alpha \in \mathcal{R}^m$ from the set*

$$\mathcal{C}_T = \{a\alpha \mid \alpha \in \mathcal{G} \cup \mathcal{H}, a \in \mathcal{M} \text{ and } \mathfrak{s}(a\alpha) = T\}. \quad (2)$$

Usually the Rewritten criterion as stated above is only defined for $\alpha \in \mathcal{G}$. The second criterion is then the so-called **F5 criterion** or *Syzygy criterion*. This criterion states that whenever the signature of an S-pair is a multiple of the lead term of a syzygy in \mathcal{R}^m , then the pair can be removed. $\alpha \in \mathcal{H}$ means that α is a syzygy and its signature is equal to the lead term in \mathcal{R}^m . Clearly, whenever in

¹Since we assume that the reader is more familiar with the installation of Gebauer and Möller than with signature-based Gröbner basis algorithms we only present the pseudo code of **RB** in Algorithm 1.

Algorithm 1 RB (Rewrite Basis Algorithm)

Require: Ideal $I = \langle f_1, \dots, f_m \rangle \subset \mathcal{R}$, monomial order \leq on \mathcal{R} and a compatible extension on \mathcal{R}^m , a rewrite order \preceq on $\mathcal{G} \cup \mathcal{H}$

Ensure: Signature Gröbner basis \mathcal{G} for I , Gröbner basis \mathcal{H} for $\text{syz}(f_1, \dots, f_m)$

```
1:  $\mathcal{G} \leftarrow \emptyset, \mathcal{H} \leftarrow \emptyset$ 
2:  $\mathcal{P} \leftarrow \{e_1, \dots, e_m\}$ 
3:  $\mathcal{H} \leftarrow \{f_i e_j - f_j e_i \mid 1 \leq i < j \leq m\} \subset \mathcal{R}^m$ 
4: while  $\mathcal{P} \neq \emptyset$  do
5:    $\beta \leftarrow$  element of minimal signature w.r.t.  $\leq$  from  $\mathcal{P}$ 
6:    $\mathcal{P} \leftarrow \mathcal{P} \setminus \{\beta\}$ 
7:   if not Rewritable( $\beta, \mathcal{G} \cup \mathcal{H}, \preceq$ ) then
8:      $\gamma \leftarrow$  result of regular  $s$ -reducing  $\beta$ 
9:     if  $\bar{\gamma} = 0$  then
10:       $\mathcal{H} \leftarrow \mathcal{H} + \{\gamma\}$ 
11:   else
12:      $\mathcal{P} \leftarrow \mathcal{P} \cup \{\text{spair}(\alpha, \gamma) \mid \alpha \in \mathcal{G}, \text{spair}(\alpha, \gamma) \text{ regular}\}$ 
13:      $\mathcal{G} \leftarrow \mathcal{G} \cup \{\gamma\}$ 
14:     UpdateSyz( $\mathcal{G}, \mathcal{H}$ )
15: return ( $\mathcal{G}, \mathcal{H}$ )
```

Algorithm 2 Rewritable (Rewritten Criterion Check)

Require: S-pair $a\alpha - b\beta \in \mathcal{R}^m$

Ensure: “true” if S-pair is rewritable; else “false”

```
1: if  $a\alpha$  is rewritable then
2:   return true
3: if  $b\beta$  is rewritable then
4:   return true
5: return false
```

a situation such that $\alpha \in \mathcal{H}$ and $a\alpha \in \mathcal{C}_T$ we choose $\alpha \in \mathcal{H}$ in \mathcal{C}_T , since then we do not need to do any computation in signature $T = \mathfrak{s}(a\alpha)$.

The choice in Lemma 3.3 depends on a rewrite order \preceq :

Definition 3.1. A rewrite order \preceq is a total order on \mathcal{G} such that $\mathfrak{s}(\alpha) \mid \mathfrak{s}(\beta) \Rightarrow \alpha \preceq \beta$.

Thus it makes sense to choose $\max_{\preceq} \mathcal{C}_T$ in Lemma 3.3 and remove all other corresponding S-pairs in signature T during the computations of **RB**.

Definition 3.2. We call $\delta := \max_{\preceq} \mathcal{C}_T$ the canonical rewriter in signature T w.r.t. \preceq . If $\mathfrak{s}(a\alpha) = T$ but $a\alpha$ is not the canonical rewriter in T w.r.t. \preceq then we say that $a\alpha$ (or α) is rewritable (in signature T w.r.t. \preceq). If $\delta \in \mathcal{H}$ then we say that $a\alpha$ (or α) is rewritable w.r.t. \mathcal{H} . Analogously, if $\delta \in \mathcal{G}$, we use the notation *rewritable w.r.t. \mathcal{G}* .

Two different rewrite orders are used widely these days. For both it holds that $\alpha \preceq \beta$ for $\alpha \in \mathcal{G}, \beta \in \mathcal{H}$. This condition defines the usually separately defined Syzygy criterion: Whenever we have a syzygy $\alpha \in \mathcal{H}$ such that $\mathfrak{s}(a\alpha) \mid T$ for some signature T and some multiple $a \in \mathcal{R}$ then α is the canonical rewriter. Since we already know that $\overline{\alpha} = 0$ we do not need to compute anything for signature T and can go on. To compare elements from \mathcal{G} one of the following definitions is used:

- (a) $\alpha \preceq_{\text{add}} \beta$ if α has been added to \mathcal{G} before β is added to \mathcal{G} . Break ties arbitrarily.
- (b) $\alpha \preceq_{\text{rat}} \beta$ if $\mathfrak{s}(\alpha) \text{lt}(\overline{\beta}) < \mathfrak{s}(\beta) \text{lt}(\overline{\alpha})$ or if $\mathfrak{s}(\alpha) \text{lt}(\overline{\beta}) = \mathfrak{s}(\beta) \text{lt}(\overline{\alpha})$ and $\mathfrak{s}(\alpha) < \mathfrak{s}(\beta)$.

In the following (besides the examples) we only need the general definition of \preceq . Nevertheless, the reader can think of one of the above mentioned, particular implementations if this appears to be helpful.

Remark 3.1. Note that **RB** as presented in Algorithm 1 computes not only the signature Gröbner basis \mathcal{G} for the input ideal I , but also a Gröbner basis for the corresponding syzygy module \mathcal{H} , similar to [27].

Since we are only interested in an efficient computation of \mathcal{G} it makes sense to optimize **RB**: \mathfrak{s} -reduction and the Rewritten criterion depend solely on the correctness of the signatures, the lead terms of the module representations in \mathcal{R}^m . Storing only the signature and not the full module element computations become more efficient (only reducing polynomial data, signatures are unchanged once generated), but we loose information stored in full module representation, for example, to generate more syzygies.

In the following **RB** is always assumed to use sig-poly pairs only. We want to recover as many (lead terms of) syzygies as possible without taking on the burden of computations in \mathcal{R}^m .

$\alpha_i \in \mathcal{G}$	reduced from	$\overline{\alpha_i}$	$s(\alpha_i)$
α_1	e_1	$yz - z^2$	e_1
α_2	e_2	$y^2 - xt$	e_2
α_3	e_3	$xy - xz$	e_3
α_4	e_4	$x^2 - xz$	e_4
α_5	$\text{spair}(\alpha_2, \alpha_1) = z\alpha_2 - y\alpha_1$	$z^3 - xzt$	ze_2
α_6	$\text{spair}(\alpha_3, \alpha_2) = y\alpha_3 - x\alpha_2$	$xz^2 - xzt$	ye_3

Figure 1: Computations for **RB** in Example 4.1.

Since we use the names of the above mentioned criteria a lot in the following let us agree on the following shorthand notations.

Notation 3.1. We denote the Product criterion by **PC**, the Chain criterion by **CC** and the Rewritten criterion by **RC**.

4 Improving RC

In this section we want to see how **RC** depends on the number of known syzygies **RB** can use. We show how one can use **UpdateSyz** to improve the prediction of zero reductions. For this, let us first take a look at an example using **RB**.

Example 4.1. Let \mathcal{K} be the finite field with 7 elements and let $\mathcal{R} = \mathcal{K}[x, y, z, t]$. Let $<$ be the graded reverse lexicographical monomial order which we extend to $<_{\text{lt-pot}}$ on \mathcal{R}^4 . Consider the input ideal I generated by $f_1 = yz - z^2$, $f_2 = y^2 - xt$, $f_3 = xy - xz$ and $f_4 = x^2 - xy$. We present the calculations done by **RB** using \leq_{rat} in Figure 1.

RB computes 5 zero reductions corresponding to the following syzygies:

$$\begin{aligned}
\sigma_1 &= (y + z)\alpha_4 - (x - y)\alpha_3, & \sigma_2 &= (y - z)\alpha_5 - (z^2 - xt)\alpha_1, \\
\sigma_3 &= (y - z)\alpha_6 - (z^2 - zt)\alpha_3, & \sigma_4 &= (x - y)\alpha_6 - (z^2 - zt)\alpha_4, \\
\sigma_5 &= (x^2 - xz)\alpha_5 - (z^3 - xzt)\alpha_4.
\end{aligned}$$

Note that **RB** using $<_{\text{pot}}$ or $<_{\text{d-pot}}$ computes the same example with 4 zero reductions, respectively. Even SINGULAR's [7] Gröbner basis implementation (Gebauer-Möller installation) misses only 4 zero reductions, so we must be able to improve the prediction for **RB** by using **UpdateSyz**. The idea is to implement **UpdateSyz** in a way to recover more known syzygies without blowing up \mathcal{H} too much by possibly adding redundant elements:

Algorithmic characteristic 4.1. Possible implementations of **UpdateSyz** are depending on the module monomial order $<$:

- (a) With $<_{\text{pot}}$ **RB** computes \mathcal{G} by increasing module indices. Thus, once an element γ of index k is added to \mathcal{G} such that $k > \max \{\text{ind}(\alpha) \mid \alpha \in \mathcal{G} \setminus \{\gamma\}\}$ then all new elements have index k and \mathcal{G} is a signature Gröbner basis for the input up to index $k - 1$. So we can add all syzygies $\bar{\alpha}\gamma - \bar{\gamma}\alpha$, $\alpha \in \mathcal{G} \setminus \{\gamma\}$ resp. signatures $\text{lt}(\bar{\alpha})\gamma$ to \mathcal{H} . In this way, if the input forms a regular sequence, **RB** using $<_{\text{pot}}$ does not compute any zero reduction.
- (b) For $<_{\text{lt-pot}}$ and $<_{\text{d-pot}}$ we implement **UpdateSyz** such that whenever an element γ is added to \mathcal{G} we add all syzygies $\bar{\alpha}\gamma - \bar{\gamma}\alpha$, $\alpha \in \mathcal{G} \setminus \{\gamma\}$ resp. signatures $\text{lt}(\bar{\alpha})\gamma$ to \mathcal{H} that increase $L(\mathcal{H})$. Note that in this situation we do not need to take care of the connection between $\text{ind}(\gamma)$ and $\text{ind}(\alpha)$ since this time we might have a non-incremental computation.

Using **UpdateSyz** as explained in Characteristic 4.1 **RB** behaves way better in Example 4.1: For $<_{\text{pot}}$ resp. $<_{\text{d-pot}}$ we receive 2 zero reductions. Since the input is homogeneous the number of zero reductions for $<_{\text{pot}}$ and $<_{\text{d-pot}}$ coincides.²

For $<_{\text{lt-pot}}$ we only drop from 5 to 3 syzygies: σ_2 and σ_3 are now detected in **Rewritable** due to additional elements in \mathcal{H} .

Remark 4.1. Note that one can optimize \mathcal{H} even further when more algebraic structure of the input is known. For example, in [12], bihomogeneous input is investigated. Using this fact one can construct even more syzygies or relations by taking information about the corresponding Jacobian matrices into account.

5 RC covers CC

Looking at equations 1 and 2 it seems that there is a strong connection between both criteria. In [16] Gash shortly discusses the possibility of adding **CC** to **F5** in special situations. Here we show that **RC** completely covers **CC** and thus need not be added to **RB** (or **F5** as a specific implementation of it).

Theorem 5.1. *Let $\alpha, \beta, \gamma \in \mathcal{R}^m$ such that $(\bar{\alpha}, \bar{\beta}, \bar{\gamma})$ fulfills **CC**. Then **RC** removes one of the corresponding *S*-pairs $\text{spair}(\alpha, \beta)$, $\text{spair}(\alpha, \gamma)$ resp. $\text{spair}(\gamma, \beta)$.*

²Note that for affine input this need not be the case due to possible degree drops during the computation of \mathcal{G} .

Proof. Since $(\bar{\alpha}, \bar{\beta}, \bar{\gamma})$ fulfills **CC** there exist by Equation 1 monomials $u, v \in \mathcal{M}$ such that

$$\overline{\text{spair}(\alpha, \beta)} = u \overline{\text{spair}(\alpha, \gamma)} + v \overline{\text{spair}(\gamma, \beta)}. \quad (3)$$

For corresponding monomial multiples this corresponds, on the polynomial side, to

$$a_\beta \bar{\alpha} - b_\alpha \bar{\beta} = u (a_\gamma \bar{\alpha} - c_\alpha \bar{\gamma}) + v (c_\beta \bar{\gamma} - b_\gamma \bar{\beta})$$

such that $a_\beta = ua_\gamma$, $b_\alpha = vb_\gamma$ and $uc_\alpha = vc_\beta$. This has the effect that the corresponding multiplied signatures coincide, too. $\mathcal{T} := \{s(a_\beta \alpha), s(b_\alpha \beta), s(uc_\alpha \gamma)\}$ denotes the set of all appearing signatures. It follows that $\max_{<} \mathcal{T}$ appears twice in Equation 3.³ Thus, depending on u and v one of the two S-pairs with maximal signature is detected by **RC** due to the other one. \square

Theorem 5.1 states that whenever an S-polynomial would be discarded by **CC**, then the corresponding S-pair is removed by **RC**. Thus, a signature-based Gröbner basis algorithm implementing **RC** as stated in Lemma 3.3 includes **CC**.

Remark 5.1.

- (a) Depending on u and v one has a choice which of the three S-polynomials fulfilling **CC** can be removed. In a signature-based Gröbner basis algorithm the chosen rewrite order \leq uniquely defines the S-pair to be discarded in such a situation.
- (b) **CC** corresponds to a found syzygy. The problem for an efficient implementation of a signature-based Gröbner basis algorithm using sig-poly pairs (see Remark 3.1) is that one cannot track this syzygy: One only has the information of the signature stored. In the setting of Theorem 5.1 two module lead terms cancel out each other, that means the signatures are the same. Due to the fact that the tail of the syzygy is not stored the algorithm cannot recompute the new module lead term resp. signature that could be added to \mathcal{H} . Thus, although we can remove an S-pair corresponding to this relation in **RB** we are not able to use this information on a more global level by adding information to \mathcal{H} .

As seen in Theorem 5.1 **CC** is just a particular case of **RC**. Thus it is clear that **RC** can remove more elements than **CC**.

Example 5.1. Let \mathcal{K} be the finite field with 7 elements and let $\mathcal{R} = \mathcal{K}[x, y, z, t]$. Let $<$ be the graded reverse lexicographical monomial order which we extend to $<_{\text{pot}}$ on \mathcal{R}^3 . Consider the input ideal I generated by $f_1 = yz - 2t^2$, $f_2 = xy + t^2$, and $f_3 = x^2z + 3xt^2 - 2yt^2$. We present the calculations done by **RB** using \leq_{rat} in Figure 2.

³Note that $s(uc_\alpha \gamma) = \max_{<} \mathcal{T}$ is possible.

$\alpha_i \in \mathcal{G}$	reduced from	$\text{lt}(\overline{\alpha_i})$	$\mathfrak{s}(\alpha_i)$
α_1	\mathbf{e}_1	$y\mathbf{z}$	\mathbf{e}_1
α_2	\mathbf{e}_2	$x\mathbf{y}$	\mathbf{e}_2
α_3	$\text{spair}(\alpha_2, \alpha_1) = z\alpha_2 - x\alpha_1$	xt^2	$z\mathbf{e}_2$
α_4	\mathbf{e}_3	$x^2\mathbf{z}$	\mathbf{e}_3
α_5	$\text{spair}(\alpha_4, \alpha_2) = y\alpha_4 - xz\alpha_2$	y^2t^2	$y\mathbf{e}_3$
α_6	$\text{spair}(\alpha_4, \alpha_3) = t^2\alpha_4 - xz\alpha_3$	z^3t^2	$t^2\mathbf{e}_3$

Figure 2: Computations for **RB** in Example 5.1.

RB removes $\text{spair}(\alpha_6, \alpha_1) = y\alpha_6 - z^2t^2\alpha_1$ due to the rewriting of α_5 : $\mathfrak{s}(y\alpha_6) = \mathfrak{s}(t^2\alpha_5)$ and $\text{lt}(\overline{y\alpha_6}) = yz^3t^2 > y^2t^4 = \text{lt}(\overline{t^2\alpha_5})$. Recalculating this rewriting one gets

$$\text{spair}(\alpha_6, \alpha_1) = y\alpha_6 - z^2t^2\alpha_1 = t^2(\alpha_5 + (2y + 3z)\alpha_3 - t^2\alpha_1)$$

where $\text{lt}(\overline{\alpha_5}) > \text{lt}(\overline{y\alpha_3}) > \text{lt}(\overline{t^2\alpha_1})$. **CC** does not detect this relation, even not in an optimized Gebauer-Möller variant as implemented in **SINGULAR** ([7]). There, a reduction to zero is computed.

Remark 5.2. Any signature-based Gröbner basis algorithm implementing **RC** as discussed in sections 3 and 4 does not need any further modifications to detect the useless computations **CC** predict. This leads to an easier description of the algorithm compared to Theorem 3.1 in [19] where **CC** is explicitly added as conditions C_2 and C_3 . There Gerdt and Hashemi add a Gebauer-Möller-like criteria check to their modified **ImpG2V** algorithm.

6 Does RC cover PC, too?

As for **CC** we wish to find a connection between **RC** and **PC**. The nice fact is that we can easily translate Lemma 3.1 to the signature-based world. Note the subtle difference that the argument of Corollary 6.1 holds for regular \mathfrak{s} -reductions whereas Lemma 3.1 does not have this restriction.

Corollary 6.1 (Variant of Lemma 3.1). *Let $\alpha, \beta \in \mathcal{R}^m$ with $\text{lcm}(\text{lt}(\overline{\alpha}), \text{lt}(\overline{\beta})) = \text{lt}(\overline{\alpha})\text{lt}(\overline{\beta})$. Then $\text{spair}(\alpha, \beta)$ regular \mathfrak{s} -reduces to zero w.r.t. $\{\alpha, \beta\}$.*

Proof. Let $T = \max_{<} \{s(\text{lt}(\overline{\beta})\alpha), s(\text{lt}(\overline{\alpha})\beta)\}$. For any $u \in \sup(\overline{\beta} - \text{lt}(\overline{\beta}))$, $v \in \sup(\overline{\alpha} - \text{lt}(\overline{\alpha}))$ it holds that $s(u\alpha) < T$ and $s(v\beta) < T$. \square

The outcome of Corollary 6.1 is that in **RB PC** can be used without any further restrictions or modifications. This is something already discussed in [16, 20, 19]. With this it is clear that one can modify any signature-based Gröbner basis algorithm by adding one of the following steps:

- (a) Check **PC** explicitly as it is done, for example, in **ImpG2V** in [19] (condition C_1).
- (b) Add all possible principal syzygies to \mathcal{H} whenever a new element γ with $\overline{\gamma} \neq 0$ is added to \mathcal{G} . This is done, for example, in the 2013 revision of the **GVW** algorithm, see Step 4b(b1) in Figure 3.1 in [15].

Clearly, both of these possible optimizations add an overhead to the algorithm, for example in the second case the signatures of most of the added principal syzygies are multiples of signatures already available in \mathcal{H} . Thus one also has to interreduce \mathcal{H} in order to have efficient checks of **RC** in the following. In other words, it makes sense to ask the following more algebraic question: Does **RC** cover **PC**? If not, which ones are not covered, and how can one handle these in **RB** efficiently?

Finding answers to these questions seems to be an easy task: **PC** is based on the fact that $\overline{\beta}\alpha - \overline{\alpha}\beta \in \mathcal{R}^m$ is a syzygy. So the only question is to see if **RB** finds the corresponding signature

$$\max_{<} \{s(\text{lt}(\overline{\beta})\alpha), s(\text{lt}(\overline{\alpha})\beta)\} = \max_{<} \{\text{lt}(\overline{\beta})s(\alpha), \text{lt}(\overline{\alpha})s(\beta)\}.$$

The answer to this question is not trivial as it seems to depend in the signature-based world on the chosen module monomial order. Almost always **PC** is covered by **RC**, still one can construct counterexamples:

Example 6.1 (Example 4.1 continued). In Section 4 we have implemented **UpdateSyz** in order to strengthen **RC** by relying on more known syzygies. Still, for $<_{\text{lt-pot}}$ as module monomial order we still had 3 zero reductions not discarded in advance: $\sigma_1 = (y+z)\alpha_4 - (x-y)\alpha_3$, $\sigma_4 = (x-y)\alpha_6 - (z^2-zt)\alpha_4$ and $\sigma_5 = (x^2-xz)\alpha_5 - (z^3-xzt)\alpha_4$. We see that σ_5 can be presented as $\sigma_5 = \overline{\alpha_4}\alpha_5 - \overline{\alpha_5}\alpha_4$. This means that σ_5 corresponds to a syzygy coming from an S-pair fulfilling **PC**, $\text{spair}(\alpha_5, \alpha_4)$, which is not detected by **RC** in **RB**.

Note that **RB** using $<_{\text{pot}}$ or $<_{\text{d-pot}}$ does remove all S-pairs fulfilling **PC**. Moreover, if one slightly changes $<_{\text{lt-pot}}$ to use the variant of $<_{\text{pot}}$ that prefers the smaller indices (see note after Definition 2.1) then **RC** also covers **PC**. However, mirroring this change in the input binomials one can easily construct another system where **RB** does not remove all S-pairs fulfilling **PC** with this module monomial order.

Thus we want to use the fact that not all syzygies coming from S-pairs fulfilling **PC** are found in **RB**. Due to Corollary 6.1 we can easily implement it in **RB** without affecting correctness or termination. In order to do this efficiently, one should take a bit care: Since **RB** is a signature-based Gröbner basis algorithm its criterion, **RC**, should be favored over **PC**. Thus we might change Algorithm 2 to the variant presented in Algorithm 3.

Algorithm 3 Rewritable' (Rewritten & Product Criterion Check)

Require: S-pair $a\alpha - b\beta \in \mathcal{R}^m$

Ensure: “true” if S-pair is rewritable or fulfills the Product criterion; else “false”

- 1: **if** $a\alpha$ or $b\beta$ is rewritable w.r.t. \mathcal{H} **then**
 - 2: **return** true
 - 3: **if** $a\bar{\alpha} - b\bar{\beta}$ fulfills the Product criterion **then**
 - 4: $\mathcal{H} \leftarrow \mathcal{H} \cup \{\bar{\alpha}\beta - \bar{\beta}\alpha\}$
 - 5: **return** true
 - 6: **if** $a\alpha$ or $b\beta$ is rewritable w.r.t. \mathcal{G} **then**
 - 7: **return** true
 - 8: **return** false
-

Comparing **Rewritable'** with **Rewritable** we see first that **RC** is split up: In Line 1 we check with elements in \mathcal{H} , in Line 6 we check with elements in \mathcal{G} . Between those two tests, we check for **PC** (Line 3). In this way the overhead is minimized:

- (a) If an S-pair is already removed in Line 1 then we have already a corresponding syzygy. This happens in Example 4.1 for 5 S-pairs fulfilling **PC**.
- (b) If an S-pair was not removed in the first step, but fulfills **PC** then the corresponding syzygy $\sigma = \bar{\alpha}\beta - \bar{\beta}\alpha$ is missing in \mathcal{H} . We can remove spair (α, β) due to Corollary 6.1. Here it makes sense to add σ to \mathcal{H} since there exists no $\sigma' \in \mathcal{H} \setminus \{\sigma\}$ such that $s(\sigma') \mid s(\sigma)$.
- (c) If spair (α, β) was not removed in the first two steps, we check for rewriters in \mathcal{G} .

Above we said that **RB** shall favor **RC** over **PC**, so why do we check rewritability w.r.t. \mathcal{G} last? The answer to this question is that being rewritable w.r.t. \mathcal{G} is a local property. At some point **RB** might have computed enough successors of elements in \mathcal{G} that a canonical rewriter in signature T might no longer be the canonical one in signature tT for some $t \in \mathcal{M}$. Thus the relation stored in this canonical rewriter is no longer available to **RB**. Having instead a new syzygy $\sigma \in \mathcal{H}$ this is a global canonical rewriter that removes useless S-pairs in any signature that is a multiple of $s(\sigma)$. So even if for $a\bar{\alpha} - b\bar{\beta}$ fulfilling **PC** $a\alpha$ or $b\beta$ is rewritable w.r.t. \mathcal{G} it makes sense to check **PC** first and add a new syzygy to \mathcal{H} as we see in Section 8.

Looking again at Example 4.1 we see that a variant of **RB** using **Rewritable'** detects spair (α_5, α_4) and adds the corresponding syzygy σ_5 without comput-

ing a zero reduction. Thus also when using $<_{\text{lt-pot}}$ **RB** predicts all except 2 zero reductions.

As a last fact let us compare the ideas behind Gebauer and Möller's implementation of **PC** and **CC** in terms of efficiency to signature-based Gröbner basis algorithms: Assume that $(\overline{\alpha}, \overline{\beta}, \overline{\gamma})$ fulfills **CC** such that $\text{lcm}(\text{lt}(\overline{\alpha}), \text{lt}(\overline{\beta})) = \text{lcm}(\text{lt}(\overline{\alpha}), \text{lt}(\overline{\gamma}))$. Now both, $\overline{\text{spair}(\alpha, \beta)}$ and $\overline{\text{spair}(\alpha, \gamma)}$ can be removed. The hard part is to not remove both at the same time. Gebauer and Möller implemented a step-by-step check of **CC** and **PC**, in order to remove useless S-polynomials as early as possible including a check to not remove both S-polynomials in the above situation. Looking at this from the signature-based point of view, $s(\overline{\text{spair}(\alpha, \beta)}) = s(\overline{\text{spair}(\alpha, \gamma)})$. Due to the rewrite order and the handling of S-pairs by increasing signature in **RB** one of the two S-pairs is handled first, say $\overline{\text{spair}(\alpha, \beta)}$. This means that (if there is no other criterion to remove it) $\overline{\text{spair}(\alpha, \beta)}$ is further reduced whereas $\overline{\text{spair}(\alpha, \gamma)}$ is rewritten. Thus it is not possible to remove too many elements in such a chain when using signature-based Gröbner basis algorithms.

Moreover, the Gebauer and Möller implementation checks **PC** last in order to remove correctly as much as possible useless S-polynomials. For example, for $(\overline{\alpha}, \overline{\beta}, \overline{\gamma})$ fulfilling

$$\overline{\text{spair}(\alpha, \beta)} = \overline{u \text{spair}(\alpha, \gamma)} + \overline{v \text{spair}(\gamma, \beta)}$$

it is possible that one removes $\overline{\text{spair}(\alpha, \beta)}$. Later on, $\overline{\text{spair}(\alpha, \gamma)}$ fulfills **PC** and is removed, too. In this situation, out of three S-polynomials only one, $\overline{\text{spair}(\beta, \gamma)}$ needs to be further reduced. In a signature-based algorithm the question whether **RC** w.r.t. \mathcal{H} detects one of these elements naturally comes up. If $s(\overline{\text{spair}(\alpha, \gamma)})$ is rewritable w.r.t. \mathcal{H} then $s(\overline{\text{spair}(\alpha, \beta)})$ is so, too. Thus also in **RB** only one S-pair would be left.

7 Covering PC in RBA using $<_{\text{pot}}$

An astonishing point is the fact that when **RB** uses $<_{\text{pot}}$ we have not found any example where an S-pair fulfilling **PC** is not already rewritable w.r.t. \mathcal{H} . Moreover, this behaviour seems to not depend on the ideal at all since we tried millions of examples from homogeneous to affine, from zero to higher dimensional. In all cases it holds that when using **Rewritable'** in **RB** **PC** was not used once to remove an S-pair. Let us take a more detailed look at this situation:

$<_{\text{pot}}$ enforces **RB** to compute incrementally: For each i a signature Gröbner basis \mathcal{G}_i for $\langle f_1, \dots, f_i \rangle$ is computed. Afterwards f_{i+1} enters the computations and new S-pairs are handled until a signature Gröbner basis for $\langle f_1, \dots, f_{i+1} \rangle$

is achieved. With the ideas of [8] we can assume to have the reduced Gröbner basis $\overline{\mathcal{G}}_i = \{\overline{e}_1, \dots, \overline{e}_{k-1}\} \subset \mathcal{R}$ for $\langle f_1, \dots, f_i \rangle$ before adding f_{i+1} to the computations. Assuming further to compute in the next incremental step a signature Gröbner basis for $\langle \overline{e}_1, \dots, \overline{e}_{k-1}, f_{i+1} \rangle$, we can adjust notations by setting $f_{i+1} = \overline{e}_k$. Due to the fact that $\overline{\mathcal{G}}_i$ is the reduced Gröbner basis for $\langle f_1, \dots, f_i \rangle$ we have more structure to exploit. On the other hand the incremental run of **RB** itself may put a penalty on the efficiency of the computations (often **RB** performs better using $<_{\text{lt-pot}}$ instead of $<_{\text{pot}}$).

Next we assume the start at the above incremental step with e_k . We look at S-pairs in the order they are generated by **RB**: The first possibility is to built S-pairs between elements of index k and those of index $< k$ (corresponding to polynomials in $\overline{\mathcal{G}}_i$).

Lemma 7.1. *Assume $<_{\text{pot}}$. Let $\alpha, \beta \in \mathcal{R}^m$ such that $\text{ind}(\alpha) < \text{ind}(\beta)$ and $\text{spair}(\alpha, \beta)$ fulfills **PC**. Then $a\alpha$ or $b\beta$ is rewritable w.r.t. \mathcal{H} .*

Proof. $s(\text{spair}(\alpha, \beta))$ is $\text{lt}(\overline{\alpha})s(\beta)$ since $\text{ind}(\beta) > \text{ind}(\alpha)$ and we assume $<_{\text{pot}}$. By construction $\text{lt}(\overline{\alpha}) \in L(\overline{\mathcal{G}}_i)$ and $s(\beta)$ is a multiple of e_k . Due to Line 3 for Algorithm 1 there exists an element $\sigma \in \mathcal{H}$ such that $s(\sigma) \mid \text{lt}(\overline{\alpha})s(\beta)$. \square

When generating S-pairs with both generators of index k two different situations can appear: If one of the generators is e_k we can prove the following statement.

Lemma 7.2. *Assume $<_{\text{pot}}$. Let $e_k, \beta \in \mathcal{R}^m$ such that $\text{ind}(\beta) = k$ and $\overline{\text{spair}(e_k, \beta)}$ fulfills **PC**. Then $a\alpha$ or $b\beta$ is rewritable w.r.t. \mathcal{H} .*

Proof. Since $\text{ind}(\beta) = k$ and $e_k \neq \beta$, $s(\beta) = \lambda e_k$ where $\lambda > 1$. β is a successor of some initial S-pair $\text{spair}(e_k, e_j)$ for $j < k$ (possibly over several steps). The signature of this initial S-pair is $\frac{\text{lcm}(\text{lt}(\overline{e}_k), \text{lt}(\overline{e}_j))}{\text{lt}(\overline{e}_k)} e_k$. Thus $\lambda = \lambda' \frac{\text{lcm}(\text{lt}(\overline{e}_k), \text{lt}(\overline{e}_j))}{\text{lt}(\overline{e}_k)}$ for some $\lambda' \geq 1$. Furthermore, generating the S-pair $\text{spair}(e_k, \beta)$ we get

$$\begin{aligned} \text{lt}(\overline{e}_k)s(\beta) &= \text{lt}(\overline{e}_k)\lambda' \frac{\text{lcm}(\text{lt}(\overline{e}_k), \text{lt}(\overline{e}_j))}{\text{lt}(\overline{e}_k)} e_k \\ &= \lambda' \text{lcm}(\text{lt}(\overline{e}_k), \text{lt}(\overline{e}_j)) e_k = \lambda' \lambda'' \text{lt}(\overline{e}_j) e_k. \end{aligned}$$

By the same argument as in the proof of Lemma 7.1 there exists a $\sigma \in \mathcal{H}$ that is the canonical rewriter in signature $\text{lt}(\overline{e}_k)s(\beta)$. \square

Sadly, the generalization of Lemma 7.2 by replacing e_k with an arbitrary α , $\text{ind}(\alpha) = k$ remains unproven:

Conjecture 7.1. *Assume $<_{\text{pot}}$. Let $\alpha, \beta \in \mathcal{R}^m$ such that $s(\alpha) = \lambda_\alpha e_k$, $s(\beta) = \lambda_\beta e_k$ for $\lambda_\alpha, \lambda_\beta > 1$, and $\text{spair}(\alpha, \beta)$ fulfills **PC**. Then $a\alpha$ or $b\beta$ is rewritable w.r.t. \mathcal{H} .*

The difference between Conjecture 7.1 and Lemma 7.2 lies in the fact that we loose the connection between $\text{lt}(\overline{\alpha})$ and $\text{lt}(\overline{e_k})$. The main gap in the proof of the above conjecture is the following: Since we assume $<_{\text{pot}}$ all elements $\sigma \in \mathcal{H}$ with $\mathfrak{s}(\sigma) = \lambda e_k$ have $\lambda \in L(\overline{\mathcal{G}_i})$. Moreover the following holds:

- (a) $\text{lt}(\overline{\alpha}) \notin L(\overline{\mathcal{G}_i})$ since otherwise α would have been further \mathfrak{s} -reduced (all reductions with lower index elements are regular \mathfrak{s} -reductions).
- (b) For $\mathfrak{s}(\beta) = \lambda_\beta e_k$, $\lambda_\beta \notin L(\overline{\mathcal{G}_i})$. Otherwise β would not exist in \mathcal{G} since the S-pair it is reduced from would have been removed by **RC** w.r.t. \mathcal{H} .

Still, if the conjecture is true, it must hold that $\text{lt}(\overline{\alpha}) \lambda_\beta \in L(\overline{\mathcal{G}_i})$. In contrast to the proof of Lemma 7.2 it is not even clear which element from $\overline{\mathcal{G}_i}$ might have constructed the corresponding syzygy. There are examples where the canonical rewriter $\sigma \in \mathcal{H}$ could have $\mathfrak{s}(\sigma) = \text{lt}(\overline{e_j}) e_k$ whereas $\text{lt}(\overline{e_j})$ is not involved in any predecessor of α or β at all.

Remark 7.1.

- (a) Note that for regular input sequences Conjecture 7.1 is clearly true since **RB** detects all syzygies (see, for example, Corollary 3 in [11]). Moreover, there is a connection between Conjecture 7.1 and the Moreno-Socías conjecture ([28]) (paper in preparation). Solving this problem might have a big impact on Gröbner basis computations due to revealing algebraic information not used until now.
- (b) Clearly one can always add the corresponding principal syzygy as it is done, for example, in the new version of **GVW** (see Step 4b (b1) of Figure 3.1 in [15]). Still the question of the conjecture is open: Can the underlying structure of a general signature-based Gröbner basis algorithm using $<_{\text{pot}}$ already predict those zero reductions without further modifications? This is not a question of efficient implementations, but focuses on the algebraic structures hidden underneath.

Furthermore, do we get any more syzygies resp. relations when adding all principal syzygies and interreducing \mathcal{H} or are those relations already covered by an easy implementation of Algorithm 3? These are relevant questions for understanding Gröbner basis computations.

8 Experimental results

We give some experimental results, all computed over a field of characteristic 32003 with the graded reverse lexicographical monomial order $<$. All computations were done with an implementation of **RB** in **SINGULAR** (available since version 4.0.0). All examples are available under

<https://github.com/ederc/singular-benchmarks>.

Figure 3 shows the number of zero reductions for the computation of the corresponding Gröbner bases. **STD** denotes the implementation of the Gebauer-Möller installation in **SINGULAR**, “U” denotes the usage of **UpdateSyz** as explained in Characteristic 4.1, “PC” means that **RB** uses **Rewritable**⁴. For columns including “PC” the number of Product criteria is given in brackets: those not found when checking rewritability w.r.t. \mathcal{H} first, those not found by checking rewritability w.r.t. \mathcal{H} and \mathcal{G} last. Due to the discussion in Section 7 there is no difference between using **Rewritable** or **Rewritable**⁴ for **RB** with $<_{\text{pot}}$. In all examples all syzygies coming from **PC** are rewritable w.r.t. \mathcal{H} .

RC almost always covers **PC** completely, but often first by using the rewritability check w.r.t. \mathcal{G} . This means that adding the signature of $\text{spair}(\alpha, \beta)$ in such a situation enlarges \mathcal{H} and thus might strengthen **RC**. Having tested tens of millions of examples until now it is very rarely the case that an S-pair fulfilling **PC** is not detected by **RC** at all. Random systems behave like the benchmarks given in Figure 3, thus we concentrated on the easiest cases in which such situations appear: binomial ideals. For example, using $<_{\text{lt-pot}}$ for **binomial-7-4**⁴ 8 S-pairs fulfilling **PC** are not rewritable w.r.t. \mathcal{H} , but only 3 of them are not rewritable w.r.t. \mathcal{G} . Still it makes sense to add all the corresponding syzygies, since this decreases the number of zero reductions (19 to 16). This shows again the difference between the “local” rewritable w.r.t. \mathcal{G} and the “global” rewritable w.r.t. \mathcal{H} . On the other hand, even if all those S-pairs are detected by the Rewritten criterion it is sometimes useful to add the syzygies which are not in \mathcal{H} in order to decrease the number of zero reductions computed, see, for example, **katsura-11** for $<_{\text{lt-pot}}$ or affine systems like **eco-11** or **f-744** for $<_{\text{d-pot}}$. Note that for homogeneous input **RB** using $<_{\text{d-pot}}$ might rewrite S-pairs fulfilling **PC** only w.r.t. \mathcal{G} , but not w.r.t. \mathcal{H} : Due to reasons of efficiency a practical implementation of **RB** initially checks the S-pairs at their generation directly. At this point **RB** might not have completed the computation of all lower degree signature Gröbner bases. When using **Rewritable**⁴ as stated in Algorithm 1, that means first checking the S-pair before its potential s-reduction (Line 7), a Gröbner basis up to a certain degree is already computed. So **RB** with $<_{\text{d-pot}}$ behaves in the same way as **RB** with $<_{\text{pot}}$. Furthermore, note that in any case the signature-based attempt predicts many more zero reductions than the Gebauer-Möller installation.

⁴Notation **binomial-7-4** means 7 binomial generators in a ring of 7 variables, all homogeneous and of degree 4.

Benchmark	STD	RB $<_{\text{pot}}$	RB $<_{\text{lt-pot}}$		RB $<_{\text{d-pot}}$	
		U	U	U+PC	U	U+PC
cyclic-8	4284	243	771	771(17,0)	243	243(7,0)
cyclic-8-h	5843	243	771	771(17,0)	243	243(7,0)
eco-11	3476	0	614	614(770,0)	541	538(556,0)
eco-11-h	5429	502	629	608(57,0)	502	502(10,0)
f-744	589	0	248	244(99,0)	185	184(61,0)
f-744-h	1267	189	248	244(49,0)	189	189(42,0)
katsura-11	3933	0	348	304(275,0)	0	0(62,0)
katsura-11-h	3933	0	348	304(275,0)	0	0(62,0)
noon-9	25508	0	682	646(505,0)	0	0(21,0)
noon-9-h	25508	0	682	646(505,0)	0	0(21,0)
binomial-6-2	21	6	15	8(16,7)	6	6(11,0)
binomial-6-3	20	13	15	9(6,6)	13	13(4,0)
binomial-7-3	27	24	21	21(9,0)	24	24(6,0)
binomial-7-4	41	16	19	16(8,3)	16	16(5,0)
binomial-8-3	53	23	27	27(10,0)	23	23(0,0)
binomial-8-4	40	31	26	26(3,0)	16	31(0,0)

Figure 3: # zero reductions and not detected Product criteria

9 Conclusion

We have given a discussion on different attempts to predict zero reductions during Gröbner basis computations. We have seen that **CC** is covered by **RC**. Still, efficient implementations of **RB** storing only the leading term of the syzygy cannot recover the syzygy of the corresponding chain. So the global influence of the syzygy is hidden behind the locality of rewriting w.r.t. some element in \mathcal{G} . Further research in this direction is crucial.

Even though we have shown examples where **PC** is not completely covered by **RC**. These cases are very rare. We presented an easy way to make use of **PC** in **RB** without introducing overhead. For $<_{\text{pot}}$ it seems that all syzygies coming from **PC** are already in \mathcal{H} . Proving this conjecture might give further insight in relations constructed during Gröbner basis computations.

Next we investigate the connection to the ideas for generating minimal sets of critical pairs presented in [6]. Another attempt is the generalization of the concept of signatures, storing a few more module terms to recover more syzygies, but keeping the introduced computational overhead at a minimum. The discussion presented here generalized different attempts in this direction ([16, 19, 15]) and answered open questions. The intention of this paper is not to introduce a new, more efficient variant of signature-based algorithms, but to analyze and to compare the known strategies. Different views on the prediction of zero reductions may enable us to exploit more of the algebraic structures behind Gröbner basis computations.

References

- [1] Arri, A. and Perry, J. The F5 Criterion revised. *Journal of Symbolic Computation*, 46(2):1017–1029, June 2011. Preprint online at arxiv.org/abs/1012.3664.
- [2] Becker, T., Weispfenning, V., and Kredel, H. *Gröbner Bases*. Graduate Texts in Mathematics, Springer Verlag, 1993.
- [3] Buchberger, B. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, University of Innsbruck, 1965.
- [4] Buchberger, B. A criterion for detecting unnecessary reductions in the construction of Gröbner bases. In *EUROSAM '79, An International Symposium on Symbolic and Algebraic Manipulation*, volume 72 of *Lecture Notes in Computer Science*, pages 3–21. Springer, 1979.
- [5] Buchberger, B. Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory. pages 184–232, 1985.

- [6] Caboara, M., Kreuzer, M., and Robbiano, L. Efficiently computing minimal sets of critical pairs. *J. Symb. Comput.*, 38(4):1169–1190, 2004.
- [7] Decker, W., Greuel, G.-M., Pfister, G., and Schönemann, H. *SINGULAR 4-0-0 — A computer algebra system for polynomial computations*, 2014. <http://www.singular.uni-kl.de>.
- [8] Eder, C. and Perry, J. F5C: A Variant of Faugère’s F5 Algorithm with reduced Gröbner bases. *Journal of Symbolic Computation, MEGA 2009 special issue*, 45(12):1442–1458, 2010. dx.doi.org/10.1016/j.jsc.2010.06.019.
- [9] Eder, C. and Perry, J. Signature-based Algorithms to Compute Gröbner Bases. In *ISSAC 2011: Proceedings of the 2011 international symposium on Symbolic and algebraic computation*, pages 99–106, 2011.
- [10] Eder, C. and Roune, B. H. Signature Rewriting in Gröbner Basis Computation. In *ISSAC 2013: Proceedings of the 2013 international symposium on Symbolic and algebraic computation*, pages 331–338, 2013.
- [11] Faugère, J.-C. A new efficient algorithm for computing Gröbner bases without reduction to zero F5. In *ISSAC’02, Villeneuve d’Ascq, France*, pages 75–82, July 2002. Revised version from <http://fgbrs.lip6.fr/jcf/Publications/index.html>.
- [12] Faugère, J.-C., Safey El Din, M., and Spaenlehauer, P.-J. Gröbner Bases of Bihomogeneous Ideals Generated by Polynomials of Bidegree (1,1): Algorithms and Complexity. *Journal of Symbolic Computation*, 46(4):406–437, 2011. Available online 4 November 2010.
- [13] Gao, S., Guan, Y., and Volny IV, F. A new incremental algorithm for computing Gröbner bases. In *ISSAC ’10: Proceedings of the 2010 international symposium on Symbolic and algebraic computation*, pages 13–19. ACM, 2010.
- [14] Gao, S., Volny IV, F., and Wang, D. A new algorithm for computing Groebner bases (rev. 2011). <http://www.math.clemson.edu/~sgao/papers/gvw.pdf>, 2011.
- [15] Gao, S., Volny IV, F., and Wang, D. A new algorithm for computing Groebner bases (rev. 2011). http://www.math.clemson.edu/~sgao/papers/gvw_R130704.pdf, 2013.
- [16] Gash, J. M. *On efficient computation of Gröbner bases*. PhD thesis, University of Indiana, Bloomington, IN, 2008.

- [17] Gash, J. M. A provably terminating and speed-competitive variant of F5 – F5t. *submitted to the Journal of Symbolic Computation*, 2009.
- [18] Gebauer, R. and Möller, H. M. On an installation of Buchberger’s algorithm. *Journal of Symbolic Computation*, 6(2-3):275–286, October/December 1988.
- [19] Gerdt, V. P. and Hashemi, A. On the use of Buchberger criteria in G2V algorithm for calculating Gröbner bases. *Program. Comput. Softw.*, 39(2):81–90, March 2013.
- [20] Gerdt, V. P., Hashemi, A., and M.-Alizadeh, B. Involutive Bases Algorithm Incorporating F5 Criterion. *J. Symb. Comput.*, 59:1–20, 2013.
- [21] Greuel, G.-M. and Pfister, G. *A SINGULAR Introduction to Commutative Algebra*. Springer Verlag, 2nd edition, 2007.
- [22] Huang, L. A new conception for computing Gröbner basis and its applications. <http://arxiv.org/abs/1012.5425>, 2010.
- [23] Kollreider, C. and Buchberger, B. An improved algorithmic construction of Gröbner-bases for polynomial ideals. *SIGSAM Bull.*, 12:27–36, May 1978.
- [24] Kreuzer, M. and Robbiano, L. *Computational Commutative Algebra 2*. Springer Verlag, 1st edition, 2005.
- [25] Kreuzer, M. and Robbiano, L. *Computational Commutative Algebra 1*. Springer Verlag, 2nd edition, 2009.
- [26] Mayr, E. W. and Ritscher, S. Space-efficient Gröbner basis computation without degree bounds. In Éric Schost and Ioannis Z. Emiris, editor, *IS-SAC*, pages 257–264. ACM, 2011.
- [27] Möller, H. M., Mora, T., and Traverso, C. Gröbner bases computation using syzygies. In *ISSAC 92: Papers from the International Symposium on Symbolic and Algebraic Computation*, pages 320–328, 1992.
- [28] Moreno-Socías, G. *Autour de la fonction de hilbert-samuel(escaliers d’idéaux polynomiaux)*. PhD thesis, École Polytechnique, 1991.
- [29] Pan, S., Hu, Y., and Wang, B. The Termination of the F5 Algorithm Revisited. In *ISSAC 2013: Proceedings of the 2013 international symposium on Symbolic and algebraic computation*, pages 291–298, 2013.
- [30] Roune, B. H. and Stillman, M. Practical Gröbner Basis Computation. In *ISSAC 2012: Proceedings of the 2012 international symposium on Symbolic and algebraic computation*, 2012.

- [31] Roune, B. H. and Stillman, M. Practical Gröbner Basis Computation. <http://arxiv.org/abs/1206.6940>, 2012.
- [32] Sun, Y. and Wang, D. K. A generalized criterion for signature related Gröbner basis algorithms. In *ISSAC 2011: Proceedings of the 2011 international symposium on Symbolic and algebraic computation*, pages 337–344, 2011.